

CLAIMS

What is claimed is:

1 1. A method for authentication in a network, the method comprising:
2 creating a credential string which is derived from a session ID;
3 sending a UserID associated with the session ID and the credential string to a
4 software application;
5 receiving a confirmation request which includes the credential string; and
6 sending a response in reply to the confirmation request to validate the
7 credential string to authenticate the UserID.

1 2. The method of claim 1, further comprising the step of maintaining a password at a
2 portal and not sending the password to authenticate the UserID.

1 3. The method of claim 2, wherein the credential string is an encrypted hash of the
2 session ID.

1 4. The method of claim 1, further comprising the steps of:
2 performing a lightweight directory access protocol (LDAP) lookup using the
3 UserID; and

4 if the LDAP lookup confirms the UserID and the response validates the
5 credential string, returning a successful authentication reply to the software application
6 for establishing a session associated with the session ID, otherwise sending an
7 unsuccessful authentication reply to the software application.

1 5. The method of claim 1, wherein the sending of a UserID and the credential string
2 avoids at least one of sending a user's password outside of a portal server and storing
3 the password in persistent memory.

1 6. The method of claim 1, further comprising the steps of:
2 sending the UserID associated with the session ID and the credential string to
3 a software application proxy;
4 checking whether the session ID and credential string has been previously
5 received within a predetermined time period; and
6 if affirmative, initiating a security breach procedure.

1 7. The method of claim 6, wherein the security breach procedure causes the
2 termination of any session associated with the UserID.

1 8. The method of claim 1, wherein the receiving step and sending a response step is
2 performed by an authentication proxy.

1 9. A method for authenticating a user request for a software application, the method
2 comprising:

3 receiving a UserID and credential string at an authentication proxy server;
4 sending a confirmation request from the authentication proxy to a portal, the
5 confirmation request includes the credential string;
6 receiving a response at the authentication proxy for the confirmation request;
7 and
8 validating the UserID using a light weight directory access protocol (LDAP)
9 lookup request and the response.

1 10. The method of claim 9, further comprising providing a confirmation to the
2 software application if the response is affirmative and the UserID is authenticated by
3 the LDAP lookup.

1 11. The method of claim 9, further comprising creating the credential string from a
2 session ID at the portal.

1 12. The method of claim 11, further comprising encrypting the credential string.

1 13. The method of claim 12, further comprising validating the confirmation request by
2 assuring that the credential string has been received only once for confirmation at the

3 portal, otherwise, if presented more than once, performing at least one of initiating a
4 security breach procedure and notifying a software application proxy.

1 14. The method of claim 9, further comprising receiving the UserID and a password
2 during a logon to the portal, wherein the UserID is validated in the validating step and
3 the password is maintained at the portal and used to process the confirmation request.

1 15. A system for authenticating a session, comprising:
2 an authentication proxy which receives requests to authenticate a UserID and
3 credential string; and
4 a credential string validation component which receives requests to validate
5 the credential string,
6 wherein the credential string validation component checks whether the
7 credential string has been previously received for validation within a predetermined
8 time period.

1 16. The system of claim 15, wherein the authentication proxy performs lightweight
2 directory access protocol (LDAP) lookups using the UserID and sends the credential
3 string to the credential string validation component and receives a validation reply.

1 17. The system of claim 16, wherein the authentication proxy sends an affirmative
2 authentication reply to a software application when both the LDAP lookup is
3 successful and the validation reply indicates a valid credential string.

1 18. The system of claim 17, wherein the authentication proxy receives the UserID and
2 credential string from a software application.

1 19. The system of claim 15, further comprising a software application proxy which
2 receives the UserID and credential string and detects whether the UserID and
3 credential string has been previously received within a predetermined time period.

1 20. The system of claim 19, further comprising a portal to create and encrypt the
2 credential string by hashing a session ID, the portal sends the credential string and the
3 UserID to the software application proxy, and does not send a password associated
4 with the UserID.

1 21. The system of claim 15, further comprising:

2 a portal for accepting a logon by a user and for creating the credential string
3 from an associated session ID;

4 a lightweight directory access protocol (LDAP) directory for authenticating
5 UserIDs and which is accessible by the authentication proxy; and

6 a software application proxy for intercepting the UserID and credential string
7 sent by the portal for monitoring duplicate occurrences of the UserID and credential
8 string.

1 Claim 22: A computer program product comprising a computer usable medium having
2 readable program code embodied in the medium, the computer program product
3 including at least one program code to:

4 create a credential string which is derived from a session ID;

5 send a UserID associated with the session ID and the credential string to a
6 software application;

7 receive a confirmation request which includes the credential string; and

8 send a response in reply to the confirmation request to validate the credential
9 string to authenticate the UserID.